

Improving Defense Posture Through Intelligence-based Vulnerability Management

Nelrose Vloria

Product Manager, Vulnerability Mgmt

Lauren Ashley Zamora

Engineer, Vulnerability Mgmt

November 2018

The logo features a large, stylized 'S' composed of two interlocking shapes: a blue outer ring and a black inner circle. The word 'Secureworks' is written in white, sans-serif font across the center of the black circle.

Secureworks®

Classification: //Secureworks/Confidential - Limited External Distribution:

The Challenge

The logo consists of a large, dark blue circle. Inside this circle, there is a lighter blue, stylized shape that resembles a 'C' or a partial ring. The word 'Secureworks' is written in white, sans-serif font across the center of the dark blue circle.

Secureworks®

Vulnerabilities are the #1 factor in security breaches in enterprise organizations.

>1B

records are compromised
in data breaches annually

58%

of enterprise
organizations' sensitive
data was compromised
or breached in the past
12 months

41%

of external breaches
exploited some manner
of vulnerability

Organizations still struggle with vulnerability management.

99%

of vulnerabilities exploited are known by security and IT professionals for at least one year and can be remediated

53%

of security breaches in enterprise identify vulnerabilities as a factor in the breach

56%

of organizations are dissatisfied with their capabilities to analyze and prioritize vulnerabilities

Industry-Level Vulnerability Needs and Pain Points

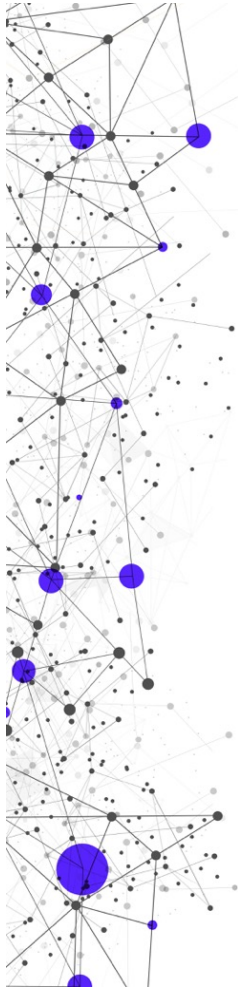
Vulnerability Needs and Pain Points		Why Current Efforts are Not Enough	
Developing ↑ ↓ Optimizing	Compliance	Government and industry regulations, such as PCI and HIPAA require a regular and active vulnerability management program. Vulnerability assessment tools are used to comply	Home Depot and Target had met their PCI compliance requirements, but they still lost payment card data
	Overwhelmed	Thousands of new vulnerabilities are introduced every year. Vulnerability managers do not have the time and resources to manage them all	Attackers exploited the unpatched Heartbleed bug at Community Health Systems (CHS) and stole around 4.5 million patients' data. The attack happened after the vulnerability was disclosed, but CHS was not able to respond fast enough
	Threat Prioritization	With limited resources, vulnerability managers need to focus on the most critical vulnerabilities	Researchers found that CVSS scores do not place enough emphasis on variables like the prevalence of exploits in the wild, leading to inaccurate assessments of criticality and wasting resources on remediating the wrong vulnerabilities
	Remediation	Remediation is painful and inefficient. Although vulnerability management and patch management go hand-in-hand, they are often managed by different teams within the organization	- This hand-off results in remediation delays. The longer the vulnerability is available, the easier it is for an attacker to stroll in. - End users want know if compensating controls can offset remediation where upgrades are prohibitively expensive
	Many Scanners	Clients often use multiple vulnerability scanners, e.g. Rapid 7 for network, WebInspect for web applications, Imperva for database, and Onapsis for SAP	These solutions tend to silo results and prevent S&R pros from getting a clear macro understanding of the vulnerabilities of high-value assets

Case Study

This case study session explains how a large services firm with limited resources worked with Secureworks for guidance on their vulnerability management program and leveraged the Qualys Cloud Platform along with Secureworks' in-house vulnerability management experts to more effectively manage and interpret their scans and prioritize remediation actions.

The logo consists of a large, dark blue circle with a lighter blue, stylized 'S' shape cut out of its center. The word 'Secureworks' is written in white, sans-serif font across the middle of the circle.

Secureworks®



Client Case Study

Challenges:

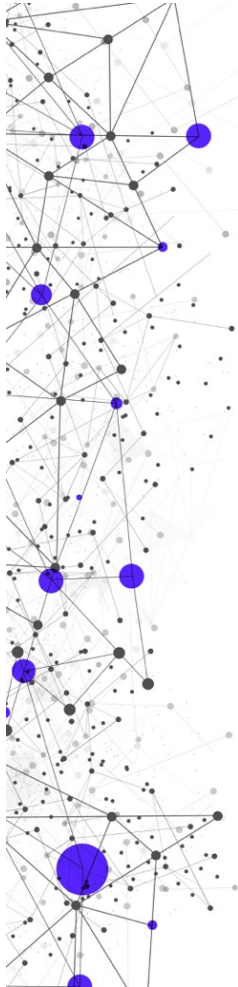
- Client was not fully leveraging the Qualys VMS platform.
- Once the client was in a weekly authenticated vulnerability scan schedule there was so much data they became overwhelmed and needed assistance with developing a reporting strategy. They needed to present the same data but in a different manner for executives, operations teams and auditors.

Solutions:

- Through a short phone call, the client learned how to leverage the Qualys VMS platform and quickly deployed authenticated scanning – revealing blind spots!

40505 Total QIDs (as of November 2018)
32625 Authenticated Only QIDs (80%)
6771 Remote Only QIDs
1077 Remote and Authenticated QIDs

- We walked the client through how to create a customized report process to suit their needs for leadership and compliance purposes.



Client Case Study

Challenges:

- The client was frustrated that there were so many vulnerabilities, that he did not know how to prioritize which threat he should tackle first.
- The client was disappointed with the lack of progress shown reducing their overall vulnerabilities detected, despite frequent remediation actions taken by their operation team.

Solutions:

- We assisted in prioritizing their vulnerabilities with a risk-based approach to focus their remediation efforts on the ones that will have the highest impact.
- We assisted the client in creating a scorecard report that showed just how effective their actions have been, and also provided ongoing tracking and reporting on progress of vulnerability remediation activities.

Other Vulnerability Management Opportunities

The logo consists of a large, dark blue circle. Inside this circle, there is a lighter blue, stylized shape that resembles a shield or a stylized 'S'. The word "Secureworks" is written in white, sans-serif font across the center of the circle.

Secureworks®

Overwhelmed

ASSUMPTION

We are just getting started and my organization has to get this vulnerability management tool up and running. It is overwhelming, and I'm on my own!

OPPORTUNITY

Our Secureworks VMS Gold team can help you co-manage your vulnerability scanner, including helping you with scheduling scans, importing asset groups, configuring reports, etc. We are also here for any questions that you might have.

Threat Prioritization

ASSUMPTION

I'm using Qualys Threat Protection to prioritize my vulnerabilities; therefore I am doing everything I can to prioritize threats.

OPPORTUNITY

Our Secureworks VMS Platinum team goes one step further by using your business context and asset criticality information to help you further prioritize remediation actions.

Program Management

ASSUMPTION

We are required to run our own vulnerability program in-house, especially because we are a large enterprise.

OPPORTUNITY

Our Secureworks VMS Platinum team can help you with fully managing your scans, analyzing reports, prioritizing threats, and working with your IT Ops teams to track their progress against critical actions.

Asset Discovery

ASSUMPTION

I discovered all my assets initially.

OPPORTUNITY

Asset discovery is not a set-it-and-forget-it feature. You should have an asset management process in place.

Patching

ASSUMPTION

I patch as I discover vulnerabilities. I am covered, right?

OPPORTUNITY

Proactive patching should be part of your security program. You do not have to wait for vulnerabilities to be identified before patching, but it helps identify CRITICAL ones that may have missed by your program.

Remediation and Executive Reporting

ASSUMPTION

Vulnerability managers are always going to have a tough time getting remediation actions completed.

OPPORTUNITY

By getting executives involved with vulnerability and remediation actions, it becomes a business and risk management decision. Our VMS Platinum team also helps track the progress of remediation actions of internal or third-party IT Ops teams.

Thank you!

Nelrose Vloria
Product Manager, Vulnerability Mgmt

Lauren Ashley Zamora
Engineer, Vulnerability Mgmt

Questions?
<https://www.secureworks.com/contact/talk-with-an-expert>

The logo features a large, stylized 'S' composed of two interlocking shapes: a blue outer ring and a black inner circle. The word 'Secureworks' is written in white, sans-serif font across the center of the black circle.

Secureworks®

Classification: //Secureworks/Confidential - Limited External Distribution: